

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Olli-Pekka POHJOLA et al.

Application No.: New Application

Filed: November 21, 2003

Attorney Dkt. No.: 60279.00073

For: SECURE UPSTREAM TRANSMISSION IN PASSIVE OPTICAL NETWORKS

CLAIM FOR PRIORITY UNDER 35 USC § 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

November 21, 2003

Sir:

The benefit of the filing dates of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

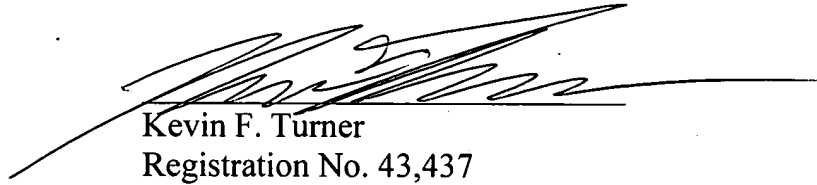
Finnish Patent Application No. 20031429 filed on October 2, 2003 in Finland

In support of this claim, a certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Please charge any fee deficiency or credit any overpayment with respect to this paper to Counsel's Deposit Account No. 50-2222.

Respectfully submitted,



Kevin F. Turner
Registration No. 43,437

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

KFT:lls

Enclosure: Priority Document (1)

PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 13.10.2003

ETUOIKEUSTODISTUS
PRIORITY DOCUMENT



Hakija
Applicant

Nokia Corporation
Helsinki

Patenttihakemus nro
Patent application no

20031429

Tekemispäivä
Filing date

02.10.2003

Kansainvälinen luokka
International class

H04B

Keksinnön nimitys
Title of invention

"Secure upstream transmission in passive optical networks"
(Varma upstream -tiedonsiirto passiivisessa optisissa verkoissa)

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä Patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.


Pirjo Kaila
Tutkimussihteeri

Maksu
Fee

50,-
50-EUR

Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1027/2001 Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.

The fee is based on the Decree with amendments of the Ministry of Trade and Industry No. 1027/2001 concerning the chargeable services of the National Board of Patents and Registration of Finland.

Osoite: Arkadiankatu 6 A Puhelin: 09 6939 500 Telefax: 09 6939 5328
P.O.Box 1160 Telephone: + 358 9 6939 500 Telefax: + 358 9 6939 5328
FIN-00101 Helsinki, FINLAND

L3

TITLE OF THE INVENTION

SECURE UPSTREAM TRANSMISSION IN PASSIVE OPTICAL NETWORKS

5 BACKGROUND OF THE INVENTION

Field of the invention:

The invention relates to communication networks and optical transmission technology. Particularly, the invention relates to Ethernet passive optical networks and improving security therein using optical disturbing reflectors.

Description of the Related Art:

In the last few years the requirements for consumer bandwidth have grown rapidly. To meet the demand for increased bandwidth new access network technologies have been developed. One such technology is based on the Institute of Electrical and Electronics Engineers (IEEE) 802.3ah standard. 802.3ah is a trademark of the IEEE inc. The standard is also known as Ethernet in the First Mile (EFM). The aim of IEEE 802.3ah is to bring Ethernet to ordinary consumers, thereby becoming an alternative for modem dial up lines and DSL connections as the primary access between a consumer and her internet service provider. The IEEE 802.3ah standard also introduces the Ethernet Passive Optical Networks (EPON) concept. The EPON is a Point-to-Multipoint (P2MP) network topology. The topology is implemented with passive optical splitters and Media Access Control (MAC) and MAC Control sublayers and physical layers that support this topology.

Reference is now made to Figure 1, which illustrates the architecture of a prior art EPON. The EPON comprises a HUB 100, to which an optical fiber 120 is connected. HUB 100 may be a passive physical

layer signal repeater or a higher protocol layer equipment such as a bridge or a router. In some contexts a HUB is also referred to as an OLT (Optical Line Terminal). For the purpose of this invention a

5 HUB such as HUB 100 is generally any kind of piece of network equipment that engages in communication with at least one optical network unit in the EPON or other equivalent medium. The optical fiber must be connected to Optical Network Units (ONU) 110, 112, 114 and 116.

10 Typically, the ONUs are located in customer premises. HUB 100 connects the EPON to an Internet Service Provider (ISP) access router or similar equipment via an upstream connection 128. In order to accomplish the connecting of HUB 100 to each of the ONUs 110-116, an

15 optical fiber 120 connects to an optical splitter 102, which connects to fibers 121 and 122. Fiber 121 connects to fibers 123 and 124 via an optical splitter 104. Finally, fiber 123 is connected to ONU 110, fiber 124 to ONU 112, a fiber 125 to ONU 114 and a fiber 126

20 to ONU 116. The direction from the ONUs 110-116 towards HUB 100 is referred to as upstream, whereas the opposite direction from HUB 100 towards the ONUs 110-116 is referred to as downstream. A signal 130, 131 transmitted from ONU 110 traverses towards HUB 100 via

25 optical splitters 104 and 102. However, a part of signal 130 may be reflected, for instance, from splitter 104 making the signal perceivable at ONU 112. Upstream and downstream signal traverses in the same fiber using different wavelengths. Other option is to have

30 separate fiber for up and downstream but this does not remove the security problem.

The drawback of the prior art IEEE 802.3ah is that the upstream traffic from any given ONU may be detectable from other ONU access points due to various

35 unwanted signal reflections. The unwanted signal reflections may not be removed or even noticed from the network beforehand. The problem is further illustrated

in Figure 2. An ONU 202 transmits a signal 220 that is to be received exclusively by a HUB 230. Along the transmission path from ONU 202 to HUB 230, there is at least a first fiber 212, an optical splitter 200 and a second fiber 210. Fiber 210 connects to at least two fibers 212 and 214 by means of optical splitter 200. Associated with fiber 210 is also a reflecting element 206, which reflects part of signal 220 as a reflection 222, which is an unwanted reflection. Reflection 222 is in turn split at optical splitter 200 and becomes perceivable at an ONU 204. Reflecting element 206 can be, for instance, a fiber connector, a fiber breaking point, an open fiber end or a second splitter along the fiber path between ONU 202 and HUB 220. Reflecting elements where discrete back reflections may occur cause privacy and confidentiality problems in EPONs. The most critical places in EPONs are on the upstream side of the splitter that is closest to the transmitting user.

In order to overcome these problems various solutions have been proposed in prior art. One such solution is to use encryption for the upstream data traffic, for instance, so that an encrypted point-to-point data link layer connection is formed between HUB 230 and transmitting ONU 202. The encryption may be based on a symmetric encryption method or an asymmetric encryption method. However, due to the point-to-multipoint nature of EPONs, the downstream traffic from HUB 230 to a given ONU may be encrypted in order to prevent eavesdropping by other ONUs connected to the same EPON[MLA5][OPH6]. The key exchange mechanisms to be used in the case where the upstream connection cannot be regarded as secure, are vastly more complicated compared to the case where the upstream connection can be regarded as reliable. By a secure connection in this case is meant a connection supporting privacy and confidentiality. More complicated mecha-

nisms always leads to the consumption of processing capacity e.g. in ONUs 202, 204 and delays in transmission. Encryption is not a mandatory feature as such in EPON. In some implementations the system could be used
5 without encryption.

An example of a key exchange mechanism to be used when the upstream connection is not reliable is the Diffie-Hellman protocol, which is disclosed e.g. in IETF RFC 2631. If the upstream connection is se-
10 cure, the establishing of a secure downstream connection from e.g. HUB 230 to ONU 202 is rather easy e.g. it is sufficient to transmit a shared secret or encryption key from ONU 202 to HUB 230 prior to downstream signal transmission.

15 If separate fiber is used for up and downstream optical isolators can be used to overcome the security problems. This is rather expensive solution.

PURPOSE OF THE INVENTION

20 The purpose of the invention is to solve the problems discussed before. Particularly, the purpose of the invention is to ensure secure and confidential upstream data transmission in Ethernet passive optical networks.

25

SUMMARY OF THE INVENTION:

The invention discloses a method for ensuring confidentiality of signal transmission in a point-to-multipoint data transmission network comprising at
30 least one hub, at least one transmission medium and at least one station connected to the hub via the at least one transmission medium. In the method an upstream signal is transmitted from a first station. The upstream signal is reflected by at least one disturbing
35 ing reflector for producing a disturbing reflection and the disturbing reflection is combined with a sec-

ond reflection of the upstream signal to render the second reflection undecodable by a second station.

5 The invention discloses also a system for ensuring confidentiality of signal transmission in a point-to-multipoint data transmission network comprising at least one hub, at least one transmission medium and at least one station connected to the hub via the at least one transmission medium. The disclosed system further comprises at least one disturbing reflector
10 placed upstream of a station and a possible point of eavesdropping, for producing a disturbing reflection of a signal transmitted by the station. The disturbing reflection combines with a second reflection of the signal.

15 The invention also discloses a network, comprising at least one hub, transmission medium and at least one station connected to the hub via the transmission medium. The data transmission network further comprises at least one disturbing reflector placed upstream of a station and a possible point of eavesdropping
20 in the transmission network for producing a disturbing reflection of a signal transmitted by the station. The disturbing reflection combines with a second reflection of the signal.

25 The invention also discloses a transmission apparatus comprising at least one optical splitter and at least one connector for an optical network unit. The transmission apparatus further comprises at least one disturbing reflector placed upstream of a station
30 and a possible point of eavesdropping in the transmission network for producing a disturbing reflection of a signal transmitted by the station. The disturbing reflection combines with a second reflection of the signal.

35 The disturbing reflector is beneficially located on the upstream side of a splitter, which connects the transmitting station and the station that is

eavesdropping. The disturbing reflector can be also on the upstream side of the unwanted reflection. The disturbing reflector produces a disturbing signal, which makes the detection of the unwanted reflection impossible.

In one embodiment of the invention the second reflection is an unwanted reflection. In one embodiment of the invention the reflection and combining means comprise a disturbing reflector, which produces a reflection of a signal transmitted via one of the connectors, and a splitter, which combines the signal transmitted and the reflection produced. In one embodiment of the invention the transmission medium is an optical fiber. It should be noted that by an optical fiber in this case is meant either a single physical fiber or several interconnected fibers that are connected using splitters. The transmission medium may also be any other medium, for example a coaxial cable. The transmission medium may also comprise two separate physical circuits or channels, one for upstream traffic and the other for downstream traffic. In the case where the transmission medium is an optical fiber, the data transmission network may be an Ethernet passive optical network and the stations may be optical network units. A disturbing reflector can be a long continuous reflector or combined from a number of discrete reflectors. Examples of reflectors are the Bragg reflectors. The disturbing reflectors may be located in a redundant branch of an optical splitter.

The benefits of the invention are related to the confidentiality and security of signal transmission in EPONs. The method and system is simplified since there is no need for expensive mutual key exchange algorithms. It is sufficient to provide confidentiality in the downstream transmission. Processing performance in the ONUs is saved. Similarly, the delay in the transmission of data is avoided, because the

key exchange before data transmission can be simplified or omitted.

BRIEF DESCRIPTION OF THE DRAWINGS:

5 The accompanying drawings, which are included to provide a further understanding of the invention and constitute a part of this specification, illustrate embodiments of the invention and together with the description help to explain the principles of the invention. In the drawings:

10 Fig. 1 is a block diagram illustrating a prior art solution that shows the structure and topology of an EPON,

15 Fig. 2 is a block diagram illustrating a prior art solution that shows a confidentiality and privacy problem associated with prior art EPONs,

20 Fig. 3 is a block diagram depicting a system, a network and a transmission apparatus utilizing the use of optical disturbing reflectors, in accordance with the invention.

 Fig. 4 is a block diagram illustrating the use of a disturbing reflector combined from discrete reflectors, in accordance with the invention.

25 Fig. 5 is a block diagram illustrating the use of a single long continuous reflector, in accordance with the invention.

 Fig. 6 is a block diagram depicting one embodiment of the invention utilizing a $2*N$ or $N*N$ optical splitter.

30 DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS:

 Reference will now be made in detail to the embodiments of the present invention, examples of which are illustrated in the accompanying drawings.

35 Figure 3 illustrates a block diagram depicting an EPON that utilizes one embodiment of the inven-

tion. The exemplary EPON comprises two ONUs 202, 204. ONUs 202 and 204 are connected to an optical splitter 200 that connects fiber 210 to a fiber 212 and a fiber 214. ONU 202 acts as the transmitting terminal that is transmitting a signal 220 to fiber 210. ONU 204 is causing a potential confidentiality problem for the transmission, since signal 220 is reflected back from a reflecting element 206 so that the intensity of the reflection permits reception at ONU 204 end of fiber 214. Reflecting element 206 is assumed to be a part of the EPON infrastructure, which cannot be eliminated or is too difficult and/or expensive to eliminate. Besides, its precise location or reflecting quality may be unknown. In accordance with the invention, fiber 210 is equipped with three disturbing reflectors 300, 302 and 304. The numbers of disturbing reflectors, ONUs and HUBs mentioned herein should be seen just as examples for the purposes of the description of the invention. The number of disturbing reflectors, ONUs and HUBs is thus not limited to their number in this example or any other example explained herein, but instead may vary in any embodiments or implementations of the invention. Particularly, the number of disturbing reflectors may be chosen by a network designer.

Signal 220 transmitted from ONU 204 is reflected at each of the disturbing reflectors 300, 302 and 304, thereby generating the disturbing reflections 224, 226 and 228 respectively. Transmitted signal 220 may be recoverable from a reflection 222 directly, since no other signals of sufficient intensity are combined with it. From the point of view of this embodiment, reflection 222 can be denoted as an unwanted reflection. However, at reflector 300, reflection 222 combines with a second reflection of the signal 220, which is caused by reflector 300. Due to propagation delay, the second reflection has a time displacement

from the reflection 222. Due to the time displacement, reflection signal 224 that includes reflection 222 and the second reflection is scrambled. The bits of reflection 222 and the second reflection are not aligned in time. Reflection signal 224 is further combined with a reflection of transmitted signal 220 at disturbing reflector 302 thereby generating a reflection signal 226 where signal 224 is further scrambled. Finally, reflection signal 226 is further combined with a reflection of the transmitted signal 220 at the disturbing reflector 304 resulting in a reflection signal 228. When reflection signal 228 is received at ONU 204, original signal 220 is no longer recoverable since reflection signal 228 is a combination of several reflections of original signal 220, each reflection having a different time displacement from the start of signal 220.

Figure 4 illustrates a block diagram depicting one embodiment of the invention where disturbing reflectors are implemented as discrete reflectors, for example as Bragg reflectors. An original signal 410 sent on an optical fiber 400 is reflected at three different disturbing reflectors 402, 404 and 406 inserted to an optical fiber 400. A reflected signal 412 represents a combination of each of the reflections caused by reflectors 402, 404 and 406. A pulse of original signal 410 is depicted on X-axis 421 and Y-axis 420, where Y-axis 420 represents signal intensity and X-axis 421 time. A resulting signal pulse 412 is as well depicted on X-axis 421 and Y-axis 420. The reflected signal 412 represents a sum of lower intensity reflections of original signal pulse 410. Each reflection has different time displacement from the start of original signal 410 thereby producing reflected signal 412 in which signal pulse is scrambled.

Figure 5 is illustrates a block diagram depicting one embodiment of the invention where disturb-

ing reflectors are implemented as a single long continuous reflector. An optical fiber 400 along which a signal 410 is transmitted has a long continuous reflector 500. The long continuous reflector 500 reflects signal energy of signal 410 along the whole length of long continuous reflector 500. The reflection characteristics may vary along the length of the long continuous reflector 500, thereby producing a reflection 502 of uneven intensity. When combined with an unwanted reflection of transmitted signal 410, reflection 502 will scramble the unwanted reflection thereby rendering it unrecognizable. The long continuous reflector must produce a reflection of sufficient intensity taking into consideration the intensity of the reflection to be scrambled. The intensity of reflection 502 must be sufficient at all its duration in order to prevent detection of pulses from the unwanted reflection.

Figure 6 illustrates a block diagram depicting one embodiment of the invention where disturbing reflectors are used in the context of a $2*N$ or $N*N$ optical splitter. A splitter 600 has two optical fibers 630 and 632 that lead towards two or more ONUs either directly or via one of several other splitters. Splitter 600 has an optical fiber 636 that is used for conveying upstream signals towards an eventual recipient. Optical fiber 636 is connected to some equipment or element that generates an unwanted reflection 624 of an upstream signal 610. In order to provide confidentiality in accordance with the invention, an extra optical fiber 634 from splitter 600 is equipped with three discrete disturbing reflectors 602, 604 and 606. The numbers of disturbing reflectors, ONUs, splitters and optical fibers mentioned herein should be seen just as examples for the purposes of the description of the invention. The number of disturbing reflectors, ONUs and optical fibers is thus not limited to their

number in this example, but instead may vary in any embodiments or implementations of the invention. Disturbing reflector 606 generates reflection 612. Disturbing reflector 604 generates a reflection, which
5 combines with the reflection 612 thereby producing a reflection 614. Disturbing reflector 606 generates a reflection, which combines with reflection 614 thereby producing a reflection 616. When reflection 616 combines with an unwanted reflection 624 at the splitter
10 600, a reflection 622 is thus generated in which transmitted signal 610 has been rendered indistinguishable and undecodable. An ONU or an eavesdropper will not be able to decode transmitted signal 610 from reflection 622. In addition to additive combination of
15 reflected signals, there will also be interference of optical carriers, causing beat noise due to the optical phase differences. It is obvious to a person skilled in the art that with the advancement of technology, the basic idea of the invention may be implemented in various ways. The invention and its embodiments
20 are thus not limited to the examples described above; instead they may vary within the scope of the claims.

CLAIMS:

1. A method for ensuring confidentiality of signal transmission in a point-to-multipoint data transmission network, comprising at least one hub, at least one transmission medium and at least one station connected to said hub via said at least one transmission medium, the method comprising:

transmitting an upstream signal from a first station;

reflecting said upstream signal by at least one disturbing reflector for producing a disturbing reflection; and

combining said disturbing reflection with a second reflection of said upstream signal to render said second reflection undecodable by a second station.

2. The method according to claim 1, wherein said second reflection is an unwanted reflection.

3. The method according to claim 1, wherein a transmission medium is an optical fiber.

4. The method according to claim 3, wherein said data transmission network is an Ethernet passive optical network and said station is an optical network unit.

5. The method according to claim 3, wherein said at least one disturbing reflector comprises at least one discrete reflector.

6. The method according to claim 3, wherein said at least one disturbing reflector is a long continuous reflector.

7. The method according to claim 3, wherein said at least one disturbing reflector is located in a redundant branch of an optical splitter.

8. A system for ensuring confidentiality of signal transmission in a point-to-multipoint data transmission network, comprising at least one hub, at least one transmission medium and at least one station

connected to said hub via said at least one transmission medium, the system further comprising:

5 at least one disturbing reflector placed upstream of a first station and a possible point of eavesdropping in said transmission network for producing a disturbing reflection of a signal transmitted by said first station, said disturbing reflection combining with a second reflection of said signal.

10 9. The system according to claim 8, wherein said second reflection is an unwanted reflection.

10. The system according to claim 8, wherein a transmission medium is an optical fiber.

15 11. The system according to claim 10, wherein said data transmission network is an Ethernet passive optical network and said station is an optical network unit.

12. The system according to claim 10, wherein said at least one disturbing reflector comprises at least one discrete reflector.

20 13. The system according to claim 10, wherein said at least one disturbing reflector is a long continuous reflector.

25 14. The system according to claim 10, wherein said at least one disturbing reflector is located in a redundant branch of an optical splitter.

15. A network comprising at least one hub, at least one transmission medium and at least one station connected to said hub via said at least one transmission medium, the network further comprising:

30 at least one disturbing reflector placed upstream of a first station and a possible point of eavesdropping in said transmission network for producing a disturbing reflection of a signal transmitted by said first station, said disturbing reflection combining
35 with a second reflection of said signal.

16. The network according to claim 15, wherein said second reflection is an unwanted reflection.

5 17. The network according to claim 15, wherein a transmission medium is an optical fiber.

18. The network according to claim 17, wherein said at least one disturbing reflector comprises at least one discrete reflector.

10 19. The network according to claim 17, wherein said at least one disturbing reflector is a long continuous reflector.

20. The network according to claim 17, wherein said at least one disturbing reflector is located in a redundant branch of an optical splitter.

15 21. A transmission apparatus comprising at least one optical splitter and at least one connector for an optical network unit, the transmission apparatus further comprising:

20 at least one disturbing reflector placed upstream of a first station and a possible point of eavesdropping in said transmission network for producing a disturbing reflection of a signal transmitted by said first station, said disturbing reflection combining with a second reflection of said signal.

25 22. The transmission apparatus according to claim 21, wherein said second reflection is an unwanted reflection.

30 23. The transmission apparatus according to claim 22, wherein said disturbing reflector comprises at least one discrete reflector.

24. The transmission apparatus according to claim 22, wherein said disturbing reflector is a long continuous reflector.

35 25. The transmission apparatus according to claim 22, wherein said disturbing reflector is located in a redundant branch of an optical splitter.

ABSTRACT OF THE DISCLOSURE

A method and system for ensuring confidentiality of signal transmission in a point-to-multipoint data transmission network like Ethernet passive optical network, comprising at least one hub, at least one transmission medium and at least one station connected to the hub via the transmission medium. When an upstream signal is transmitted from a first station, the upstream signal is reflected by at least one disturbing reflector for producing a disturbing reflection. The disturbing reflection combines with a second reflection of the upstream signal and renders the second reflection undecodable by a second station.

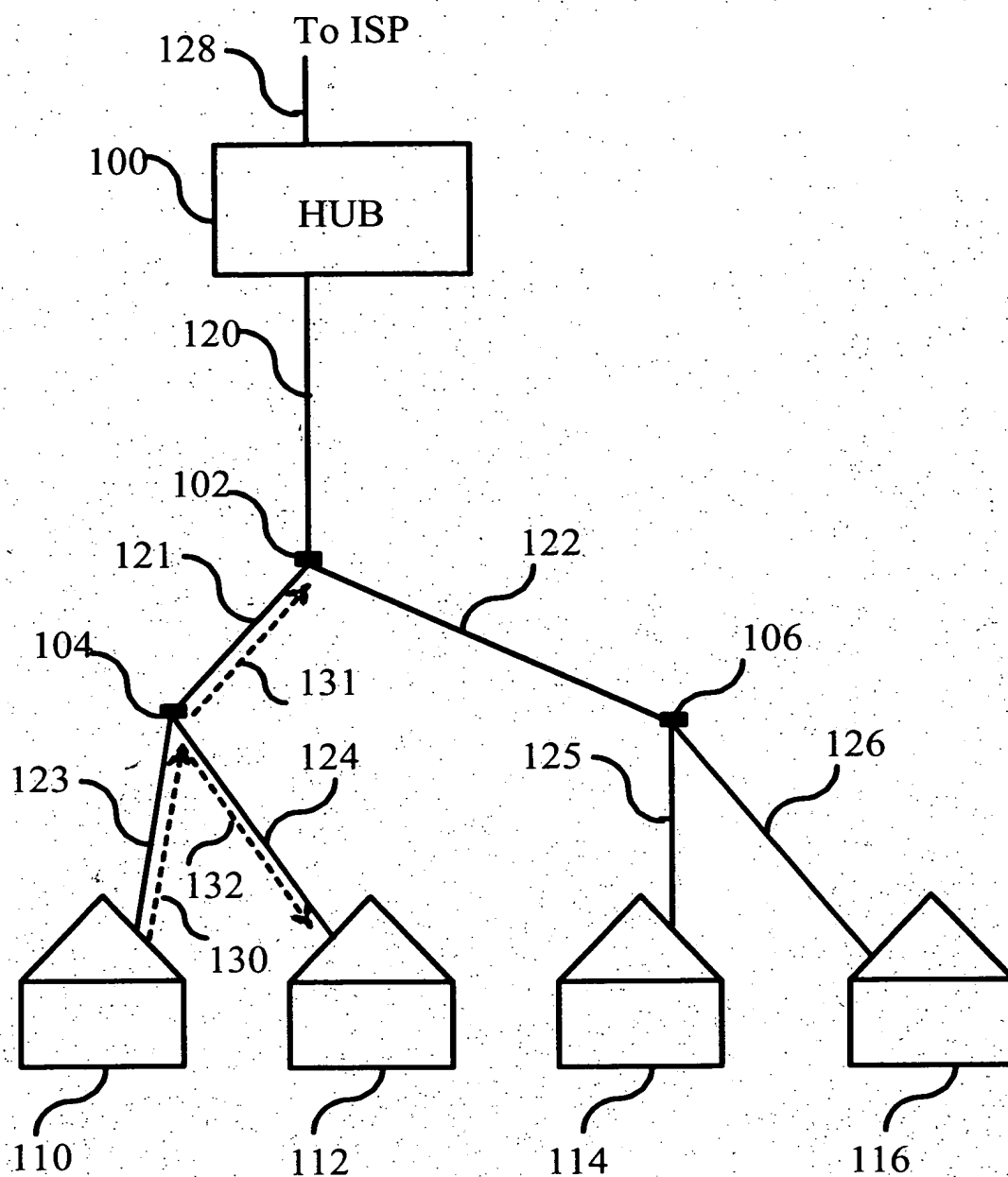


FIG .1 (PRIOR ART)

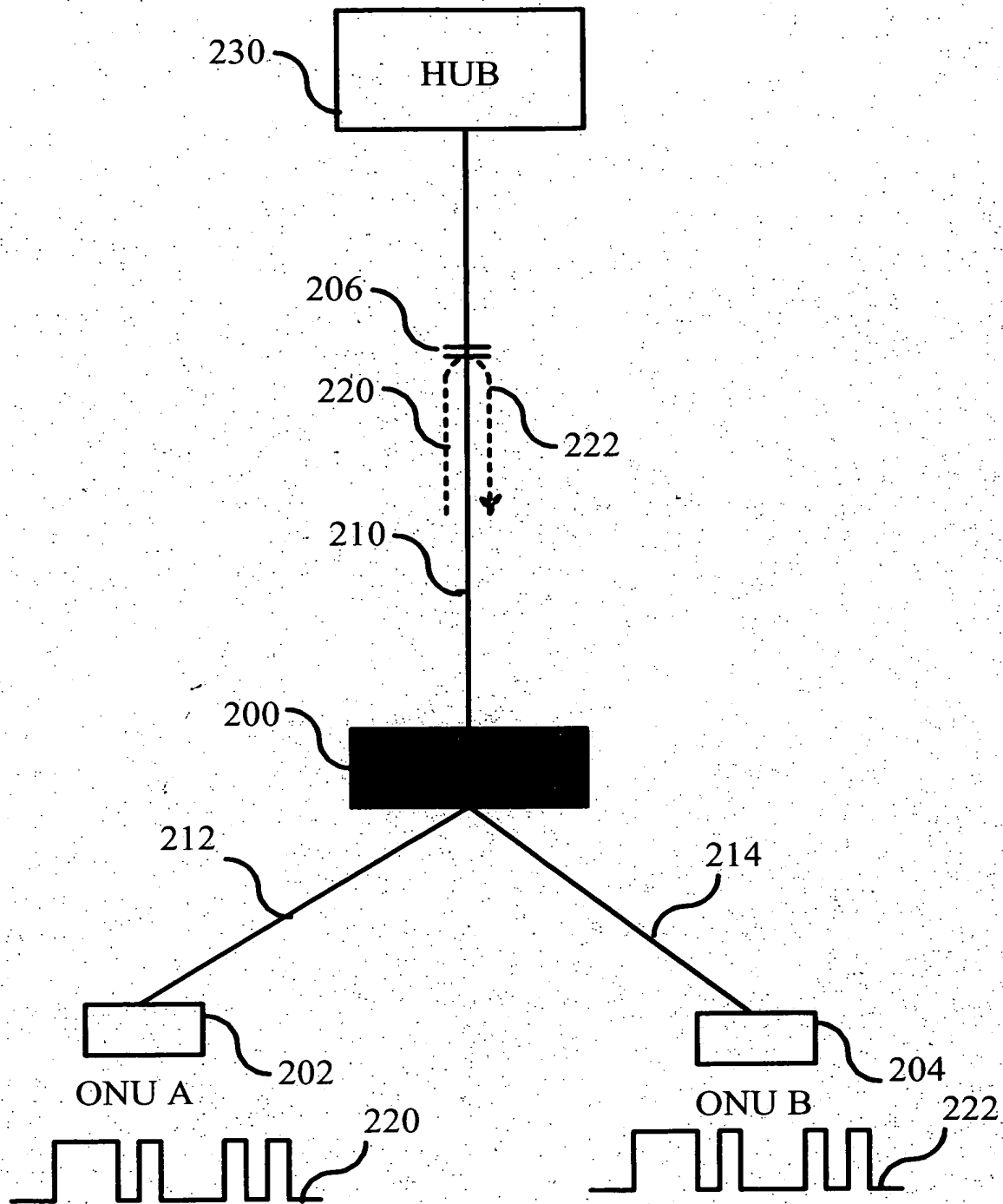


FIG. 2 (PRIOR ART)

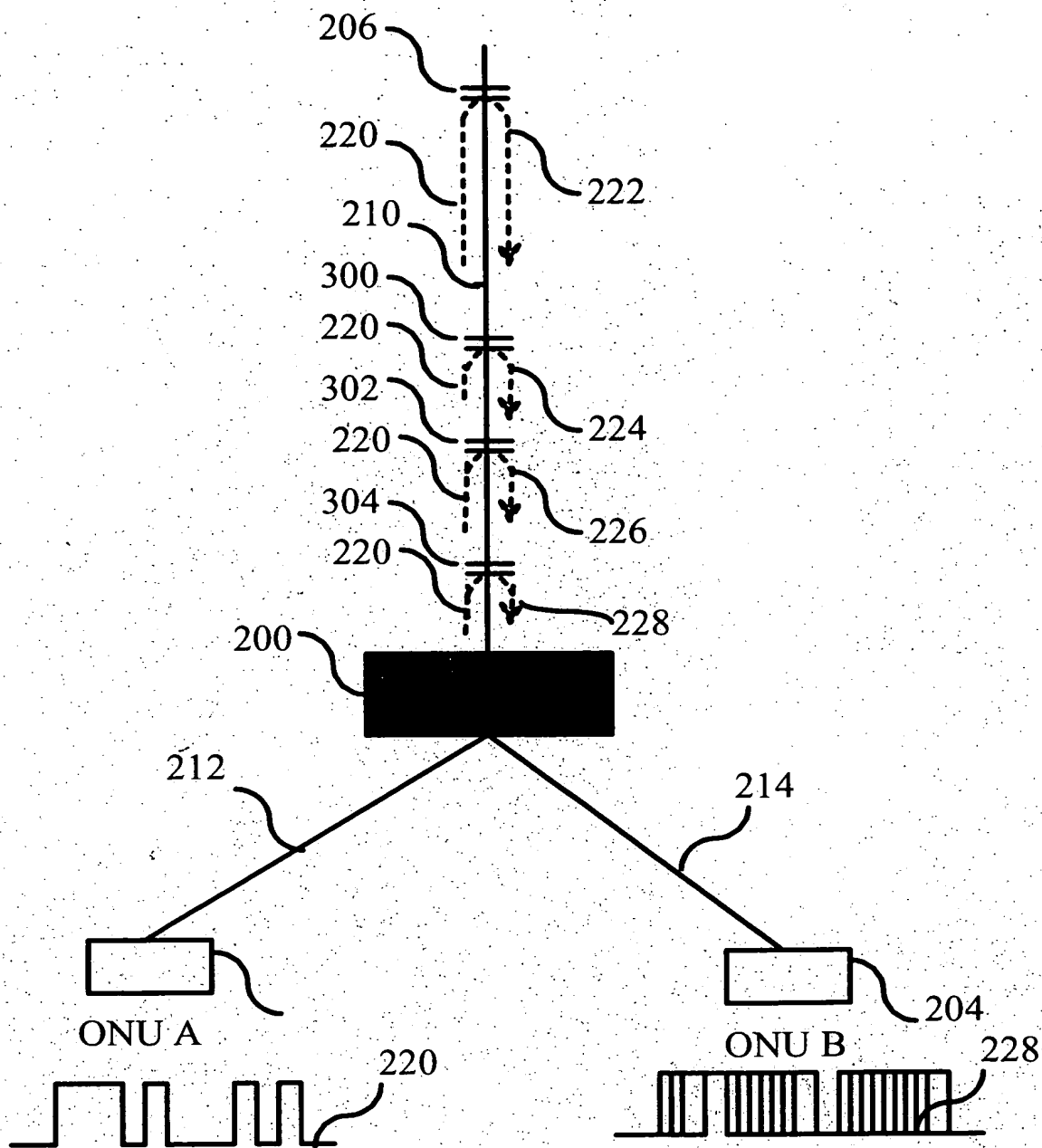
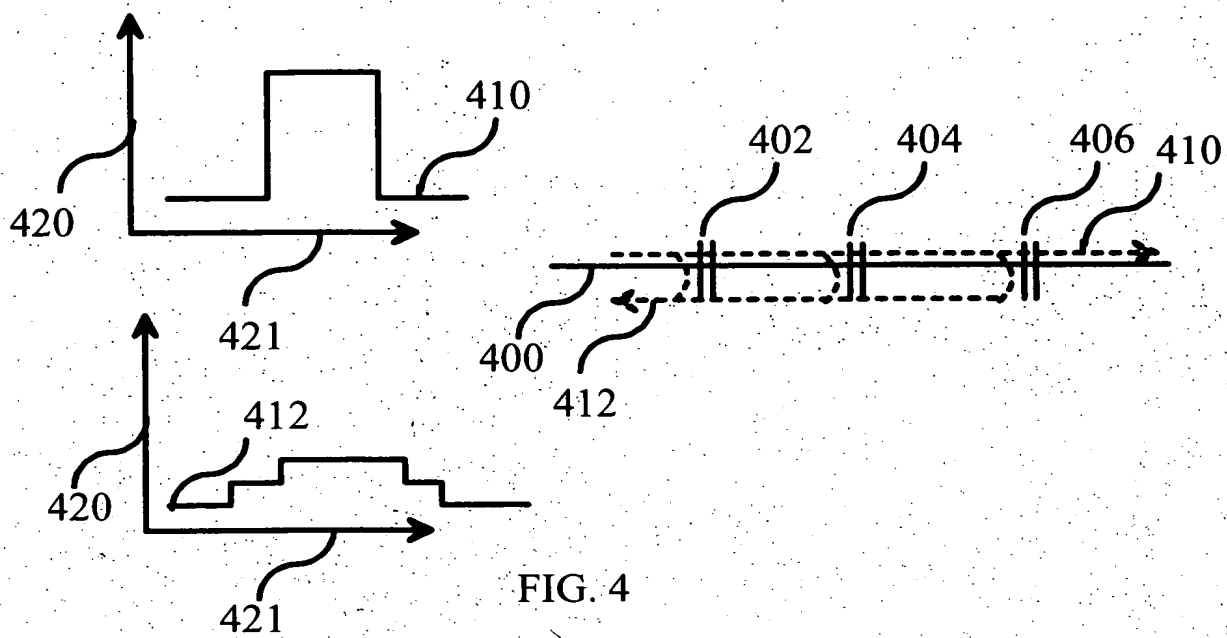
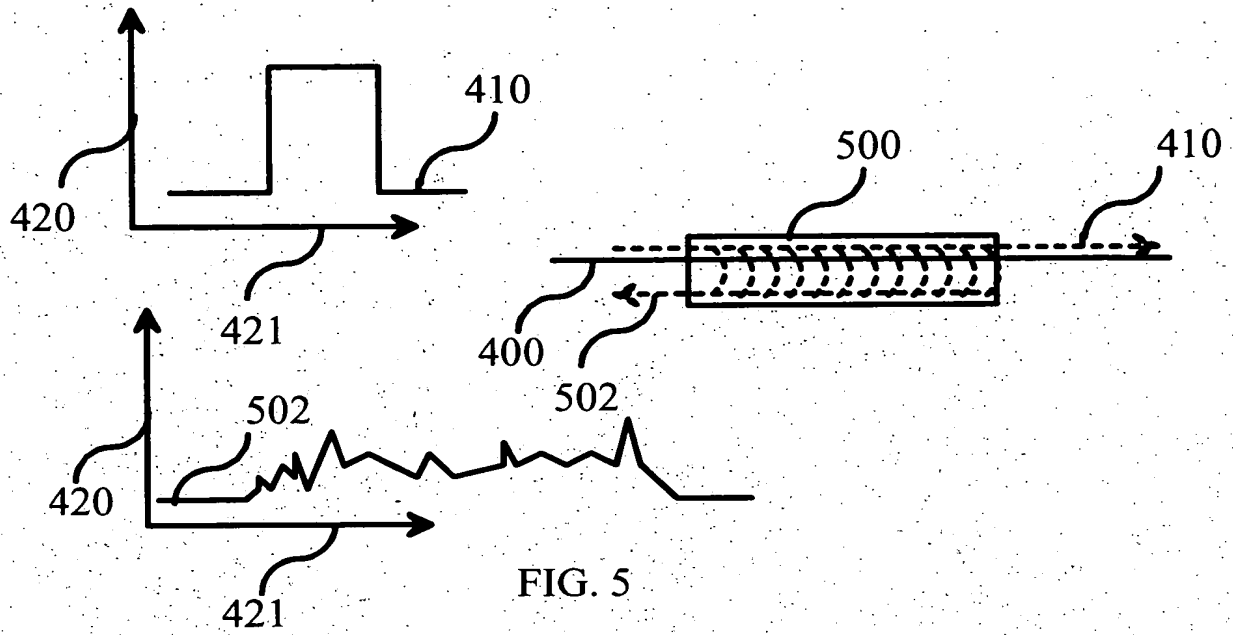


FIG. 3





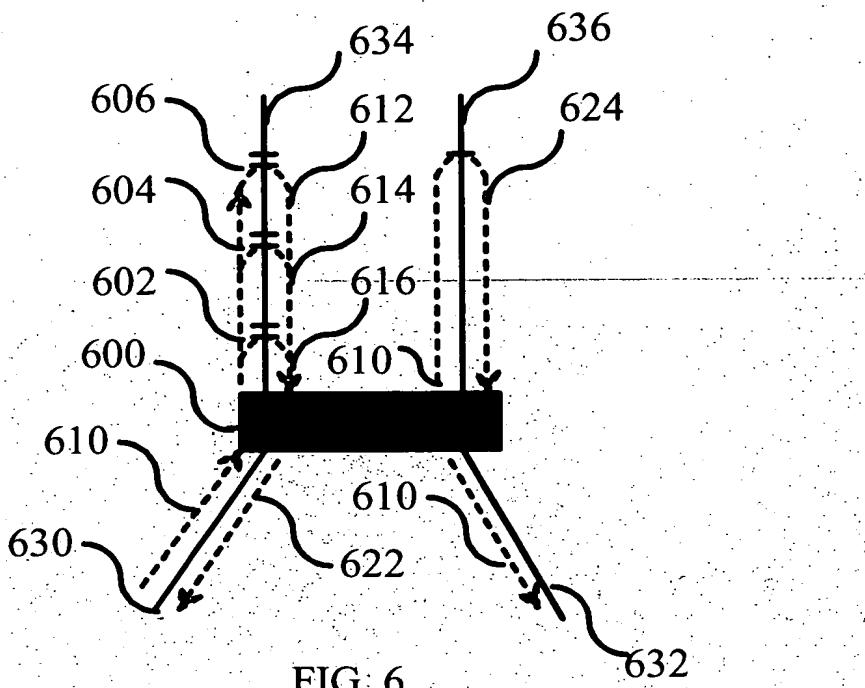


FIG. 6